In the Claims:

Please amend claims 5, 10, 24, and 30. Please add new claims 31 and 32. The claims are as follows:

1-4. (Canceled)

5. (Currently amended) A method of operating an intrusion detection system, comprising the steps of:

monitoring, by the intrusion detection system, for occurrence of a signature event that is indicative of a denial of service intrusion on a protected device, said denial of service intrusion attempting to impede operation of the protected device; and

when a signature event occurs, increasing a value of a signature event counter and comparing the value of the signature event counter with a signature threshold quantity; and

~~when~~ for each occurrence of the value of the signature event counter ~~exceeds~~ exceeding the signature threshold quantity[[,]]: generating an alert by an intrusion detection sensor of the intrusion detection system, recording a time of generating the alert in a log of a governor comprised by the intrusion detection sensor, determining from contents of the log a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold, wherein said recording is performed after said generating is performed, wherein said determining is performed after said recording is performed, and wherein said comparing the present alert generation rate with the alert generation rate threshold is performed after said determining is performed; and

~~when~~ for each occurrence of the present alert generation rate ~~exceeds~~ exceeding the alert generation rate threshold, altering an element of a signature set of the intrusion detection system to decrease an alert generation rate of the intrusion detection sensor.

6. (Previously presented) The method of claim 5, wherein the element is the signature threshold quantity.

7. (Previously presented) The method of claim 5, wherein the element is a signature threshold interval that specifies a sliding time window.

8-9. (Canceled)

10. (Currently amended) Programmable media containing programmable software for operation of an intrusion detection system, programmable software comprising the steps of:

monitoring, by the intrusion detection system, for occurrence of a signature event that is indicative of a denial of service intrusion on a protected device, said denial of service intrusion attempting to impede operation of the protected device; and

when a signature event occurs, increasing a value of a signature event counter and comparing the value of the signature event counter with a signature threshold quantity; and

~~when~~ for each occurrence of the value of the signature event counter ~~exceeds~~ exceeding the signature threshold quantity[[,]]: generating an alert by an intrusion detection sensor of the intrusion detection system, recording a time of generating the alert in a log of a governor

comprised by the intrusion detection sensor, determining from contents of the log a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold, wherein said recording is performed after said generating is performed, wherein said determining is performed after said recording is performed, and wherein said comparing the present alert generation rate with the alert generation rate threshold is performed after said determining is performed; and

~~when~~ for each occurrence of the present alert generation rate ~~exceeds~~ exceeding the alert generation rate threshold, altering an element of a signature set of the intrusion detection system to decrease an alert generation rate of the intrusion detection server.

11. (Previously presented) The programmable media of claim 10, wherein the element is the signature threshold quantity.

12. (Previously presented) The programmable media of claim 10, wherein the element is a signature threshold interval that specifies a sliding time window.

13-18. (Canceled)

19. (Previously presented) The method of claim 5, wherein said generating the alert comprises alerting an administrator of suspected denial of service intrusions upon the protected device.

20. (Previously presented) The method of claim 5, wherein the alert generation rate threshold is comprised by the governor.

21. (Previously presented) The method of claim 5, wherein the signature set comprises a unique signature set identifier, the signature event, the signature event counter, the signature threshold quantity, and a signature threshold interval that specifies a sliding time window.

22. (Previously presented) The method of claim 5, wherein the protected device is selected from the group consisting of a computer, a web server, and a workstation.

23. (Previously presented) The method of claim 5, wherein the method further comprises the step of entering into the log a list of timestamps that record the times at which the intrusion detection sensor generates alerts, wherein said determining from contents of the log a present alert generation rate utilizes the timestamps in the log.

24. (Currently amended) The method of claim 5, wherein for each occurrence of the value of the signature event counter exceeding the signature threshold quantity: after generating the alert and before determining from contents of the log the present alert generation rate, the method further comprises the step of:

clearing the log of any entries that are past a specified age.

25. (Previously presented) The programmable media of claim 10, wherein said generating the alert comprises alerting an administrator of suspected denial of service intrusions upon the protected device.

26. (Previously presented) The programmable media of claim 10, wherein the alert generation rate threshold is comprised by the governor.

27. (Previously presented) The programmable media of claim 10, wherein the signature set comprises a unique signature set identifier, the signature event, the signature event counter, the signature threshold quantity, and a signature threshold interval that specifies a sliding time window.

28. (Previously presented) The programmable media of claim 10, wherein the protected device is selected from the group consisting of a computer, a web server, and a workstation.

29. (Previously presented) The programmable media of claim 10, wherein the programmable software further comprises the step of entering into the log a list of timestamps that record the times at which the intrusion detection sensor generates alerts, wherein said determining from contents of the log a present alert generation rate utilizes the timestamps in the log.

30. (Currently amended) The programmable media of claim 10, wherein <u>for each occurrence of the value of the signature event counter exceeding the signature threshold quantity:</u> after

generating the alert and before determining from contents of the log the present alert generation rate, the programmable software further comprises the step of:

clearing the log of any entries that are past a specified age.

31 (New) The method of claim 5, further comprising the steps of:

awaiting, by the governor, for occurrence of a scheduled update time;

for each scheduled update time occurrence: clearing the log of any entries that are past a specified permissible age, determining from contents of the log the current alert generation rate, and comparing the current alert generation rate with the alert generation rate threshold; and

for each occurrence of the current alert generation rate exceeding the alert generation rate threshold: ascertaining that a signature set of the intrusion detection system is at its initial state at which no changes in the signature set have been made by the governor, and altering one or more elements of the signature set in response to said ascertaining.

32 (New) The programmable media of claim 10, wherein the programmable software further comprises the steps of:

awaiting, by the governor, for occurrence of a scheduled update time;

for each scheduled update time occurrence: clearing the log of any entries that are past a specified permissible age, determining from contents of the log the current alert generation rate, and comparing the current alert generation rate with the alert generation rate threshold; and

for each occurrence of the current alert generation rate exceeding the alert generation rate threshold: ascertaining that a signature set of the intrusion detection system is at its initial state

at which no changes in the signature set have been made by the governor, and altering one or more elements of the signature set in response to said ascertaining.